CCNA 2 v7 Modules 1 – 4: Switching Concepts, VLANs, and InterVLAN Routing Exam Answers

Question 1

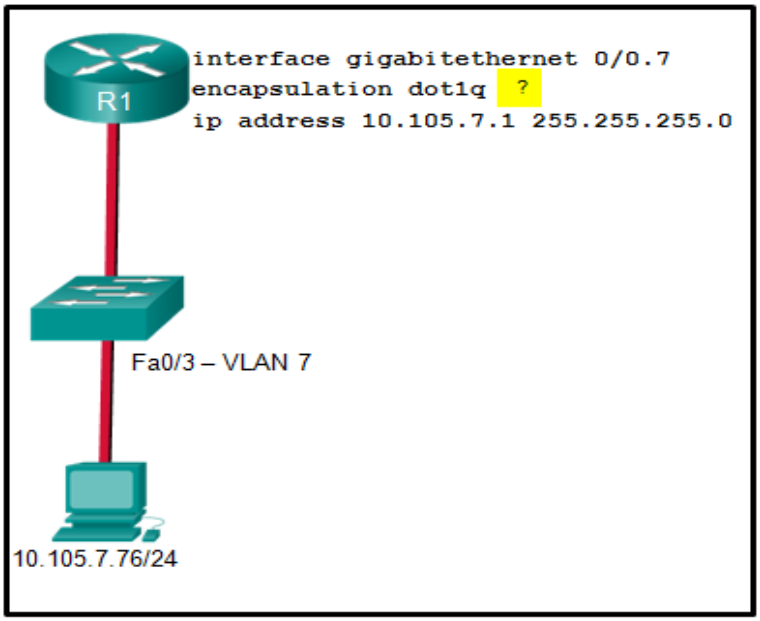
72. Which solution would help a college alleviate network congestion due to collisions?

- a firewall that connects to two Internet providers
- a high port density switch
- a router with two Ethernet ports
- a router with three Ethernet ports

Explanation: Switches provide microsegmentation so that one device does not compete for the same Ethernet network bandwidth with another network device, thus practically eliminating collisions. A high port density switch provides very fast connectivity for many devices.

Question 2

74. Refer to the exhibit. A network administrator is configuring inter-VLAN routing on a network. For now, only one VLAN is being used, but more will be added soon. What is the missing parameter that is shown as the highlighted question mark in the graphic?

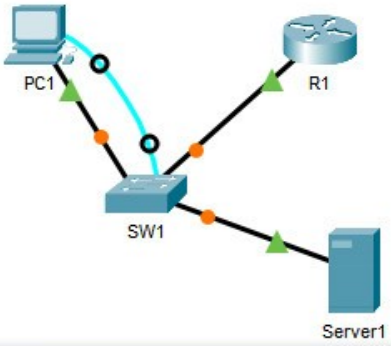


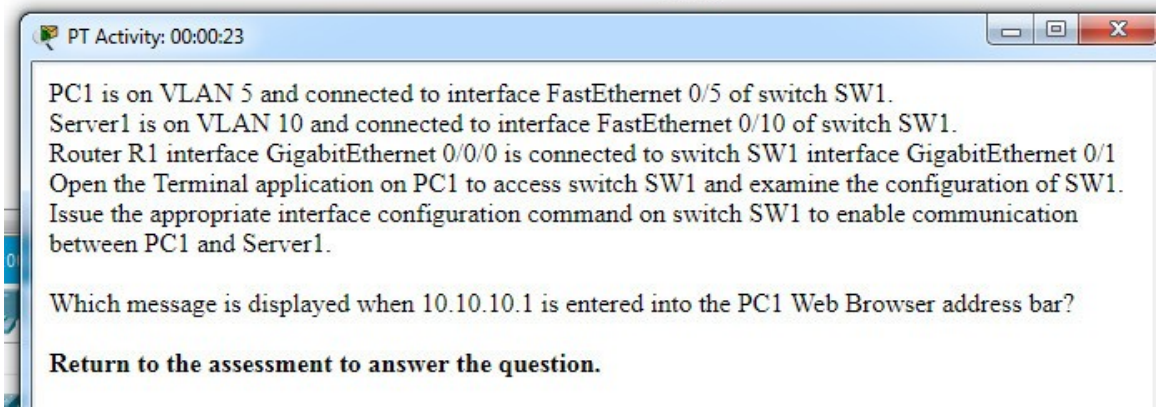
- It identifies the subinterface.
- **It identifies the VLAN number.**
- It identifies the native VLAN number.
- It identifies the type of encapsulation that is used.
- It identifies the number of hosts that are allowed on the interface.

Explanation: The completed command would be encapsulation dot1q 7. The encapsulation dot1q part of the command enables trunking and identifies the type of trunking to use. The 7 identifies the VLAN number.

Question 3

77. Open the PT Activity. Perform the tasks in the activity instructions and then answer the question.




PT Activity: 00:00:23
PC1 is on VLAN 5 and connected to interface FastEthernet 0/5 of switch SW1.
Server1 is on VLAN 10 and connected to interface FastEthernet 0/10 of switch SW1.
Router R1 interface GigabitEthernet 0/0/0 is connected to switch SW1 interface GigabitEthernet 0/1
Open the Terminal application on PC1 to access switch SW1 and examine the configuration of SW1.
Issue the appropriate interface configuration command on switch SW1 to enable communication between PC1 and Server1.
Which message is displayed when 10.10.10.1 is entered into the PC1 Web Browser address bar?
Return to the assessment to answer the question.

Which message is displayed when 10.10.10.1 is entered into the PC1 Web Browser address bar?

- Local Server
- Test Server
- **File Server**
- Cisco Server

Explanation: Examining the configuration of switch SW1 shows that interface Gi0/1 is not configured as a trunk. Issuing the interface configuration command **switchport mode trunk** on this interface will enable communications between PC1 and Server1.

Question 4

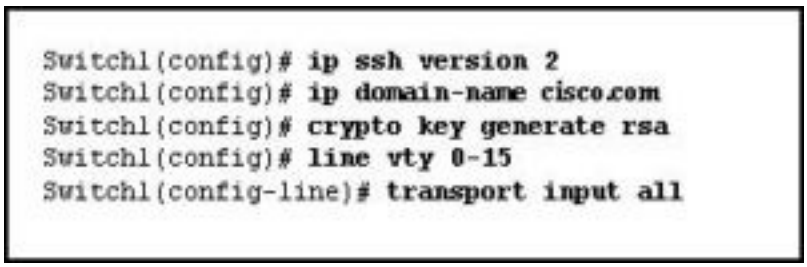
76. A network administrator issues the `show vlan brief` command while troubleshooting a user support ticket. What output will be displayed?

- the VLAN assignment and membership for device MAC addresses
- **the VLAN assignment and membership for all switch ports**
- the VLAN assignment and trunking encapsulation
- the VLAN assignment and native VLAN

Explanation: The **`show vlan brief`** command will provide information displaying the VLAN assignment and membership for all switch ports on a switch.

Question 5

71. Refer to the exhibit. The network administrator wants to configure Switch1 to allow SSH connections and prohibit Telnet connections. How should the network administrator change the displayed configuration to satisfy the requirement?


Switch1(config)# ip ssh version 2
Switch1(config)# ip domain-name cisco.com
Switch1(config)# crypto key generate rsa
Switch1(config)# line vty 0-15
Switch1(config-line)# transport input all

- Use SSH version 1.
- Reconfigure the RSA key.
- Configure SSH on a different line.
- **Modify the `transport input` command.**

Explanation: Instead of typing **`transport input all`** (which means Telnet and SSH), the network administrator should type **`transport input ssh`**.

Question 6

75. Which type of VLAN is used to designate which traffic is untagged when crossing a trunk port?

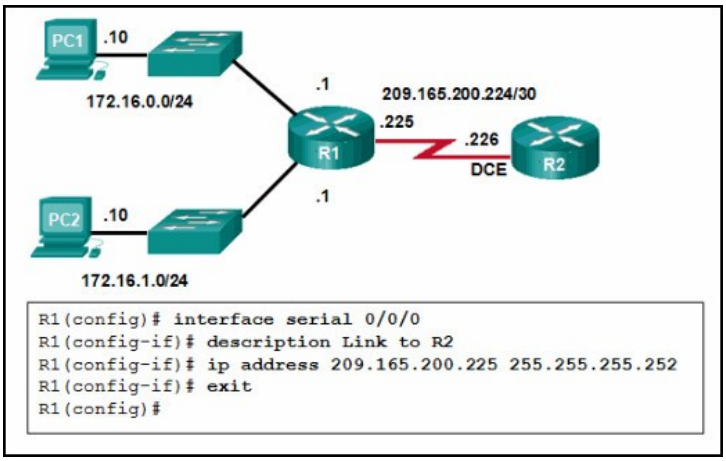
- data

- default
- **native**
- management

Explanation: A native VLAN is the VLAN that does not receive a VLAN tag in the IEEE 802.1Q frame header. Cisco best practices recommend the use of an unused VLAN (not a data VLAN, the default VLAN of VLAN 1, or the management VLAN) as the native VLAN whenever possible.

Question 7

70. Refer to the exhibit. A network administrator has configured R1 as shown. When the administrator checks the status of the serial interface, the interface is shown as being administratively down. What additional command must be entered on the serial interface of R1 to bring the interface up?



- IPv6 enable
- clockrate 128000
- end
- **no shutdown**

Explanation: By default all router interfaces are shut down. To bring the interfaces up, an administrator must issue the **`no shutdown`** command in interface mode.

Question 8

73. Which two statements are correct with respect to SVI inter-VLAN routing? (Choose two.)

- **Switching packets is faster with SVI.**
- **There is no need for a connection to a router.**
- Virtual interfaces support subinterfaces.
- SVIs can be bundled into EtherChannels.
- SVIs eliminate the need for a default gateway in the hosts.

Explanation: The SVI inter-VLAN routing method is faster than other methods. The switch can route the existing VLANs without the need for a router.

Question 9

6. If one end of an Ethernet connection is configured for full duplex and the other end of the connection is configured for half duplex, where would late collisions be observed?

- on both ends of the connection
- on the full-duplex end of the connection
- only on serial interfaces
- **on the half-duplex end of the connection**

Explanation: Full-duplex communications do not produce collisions. However, collisions often occur in half-duplex operations. When a connection has two different duplex configurations, the half-duplex end will experience late collisions. Collisions are found on Ethernet networks. Serial interfaces use technologies other than Ethernet.

Question 10

10. What is a characteristic of an IPv4 loopback interface on a Cisco IOS router?

- The no shutdown command is required to place this interface in an UP state.
- **It is a logical interface internal to the router.**
- Only one loopback interface can be enabled on a router.
- It is assigned to a physical port and can be connected to other devices.

Explanation: The loopback interface is a logical interface internal to the router and is automatically placed in an UP state, as long as the router is functioning. It is not assigned to a physical port and can therefore never be connected to any other device. Multiple loopback interfaces can be enabled on a router.

Question 11

12. After which step of the switch bootup sequence is the boot loader executed?

- after CPU initialization
- after IOS localization
- after flash file system initialization
- **after POST execution**

Explanation: The correct bootup sequence order is as follows:
1.- The switch loads and executes the POST.
2.- The switch loads the boot loader software.
3.- The boot loader performs low-level CPU initialization.
4.- The boot loader initializes the flash memory.
5.- The boot loader locates and loads the default IOS image.

Question 12

17. How do switch buffers affect network performance?

- They provide error checking on the data received.
- **They store frames received, thus preventing premature frame discarding when network congestion occurs.**
- They provide extra memory for a particular port if autonegotiation of speed or duplex fails.
- They hold data temporarily when a collision occurs until normal data transmission resumes.

Explanation: Switches have large frame buffers that allow data waiting to be transmitted to be stored so the data will not be dropped. This feature is beneficial especially if the incoming traffic is from a faster port than the egress port used for transmitting.

Question 13

18. Which switch characteristic helps keep traffic local and alleviates network congestion?

- **high port density**
- fast port speed
- large frame buffers
- fast internal switching

Explanation: Switches that have a **high port density** (=a lot of ports) reduce the number of switches required and keep some of the traffic locally on the switch, thus removing the need to send it between switches.

Question 14

15. What is the significant difference between a hub and a Layer 2 LAN switch?

- **A hub extends a collision domain, and a switch divides collision domains.**
- A hub divides collision domains, and a switch divides broadcast domains.
- Each port of a hub is a collision domain, and each port of a switch is a broadcast domain.
- A hub forwards frames, and a switch forwards only packets.

Explanation: Hubs operate only at the physical layer, forwarding bits as wire signals out all ports, and extend the collision domain of a network. Switches forward frames at the data link layer and each switch port is a separate collision domain which creates more, but smaller, collision domains. Switches do not manage broadcast domains because broadcast frames are always forwarded out all active ports.

Question 15

14. Which characteristic describes cut-through switching?

- Error-free fragments are forwarded, so switching occurs with lower latency.
- **Frames are forwarded without any error checking.**
- Only outgoing frames are checked for errors.
- Buffering is used to support different Ethernet speeds.

Explanation: Cut-through switching reduces latency by forwarding frames as soon as the destination MAC address and the corresponding switch port are read from the MAC address table. This switching method does not perform any error checking and does not use buffers to support different Ethernet speeds. Error checking and buffers are characteristics of store-and-forward switching.

Question 16

16. Which statement is correct about Ethernet switch frame forwarding decisions?

- **Frame forwarding decisions are based on MAC address and port mappings in the CAM table.**
- Cut-through frame forwarding ensures that invalid frames are always dropped.
- Only frames with a broadcast destination address are forwarded out all active switch ports.
- Unicast frames are always forwarded regardless of the destination MAC address.

Explanation: Cut-through frame forwarding reads up to only the first 22 bytes of a frame, which excludes the frame check sequence and thus invalid frames may be forwarded. In addition to broadcast frames, frames with a destination MAC address that is not in the CAM are also flooded out all active ports. Unicast frames are not always forwarded. Received frames with a destination MAC address that is associated with the switch port on which it is received are not forwarded because the destination exists on the network segment connected to that port.

Question 17

20. Refer to the exhibit. A switch receives a Layer 2 frame that contains a source MAC address of 000b.a023.c501 and a destination MAC address of 0050.0fae.75aa. Place the switch steps in the order they occur. (Not all options are used.)

```
S1# show mac-address-table
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0050.0fae.7518    DYNAMIC     Fa0/24
   2    0000.0cd1.e501    DYNAMIC     Fa0/3
   1    000b.beea.c5d4    DYNAMIC     Fa0/3
   1    00d0.d3b6.c26b    STATIC      Fa0/4
```

Occurs first **A** The switch adds the source MAC address to the MAC address table.
Occurs second **B** Because the destination is not known, the switch forwards the frame out all ports except the port through which the frame arrived.

Explanation: The first step a switch does when processing a frame is to see if the source MAC address is in the MAC address table. If the address is not there, the switch adds it. The switch then examines the destination MAC address and compares it to the MAC address table. If the address is in the table, the switch forwards the frame out the corresponding port. If the address is missing from the table, the switch will forward the frame to all ports except the port through which the frame arrived.

Question 18

19. Which switch component reduces the amount of packet handling time inside the switch?

- **ASIC**
- dual processors
- large buffer size
- store-and-forward RAM

Explanation: Application-specific integrated circuits (ASICs) are used in Cisco switches to speed up switch operations so that the switch can have an increased number of ports without degrading switch performance.

Question 19

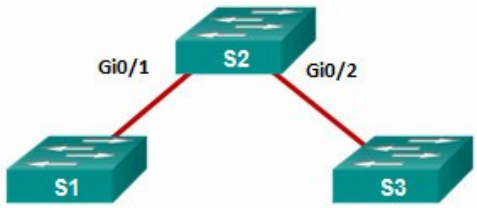
26. On a switch that is configured with multiple VLANs, which command will remove only VLAN 100 from the switch?

- Switch# delete flash:vlan.dat
- Switch(config-if)# no switchport access vlan 100
- Switch(config-if)# no switchport trunk allowed vlan 100
- **Switch(config)# no vlan 100**

Explanation: To remove all VLANs from a switch, the **`delete flash:vlan.dat`** command would be used. To change the assigned VLAN for an interface, the **`no switchport access vlan 100`** interface configuration command would be used. To remove VLAN 100 as an allowed VLAN on a trunk, the **`no switchport trunk allowed vlan 100`** would be used, but this would not remove the VLAN from the switch. To delete a single VLAN, such as VLAN 100, the **`no vlan 100`** global configuration command would be used.

Question 20

27. Refer to the exhibit. A network administrator is reviewing port and VLAN assignments on switch S2 and notices that interfaces Gi0/1 and Gi0/2 are not included in the output. Why would the interfaces be missing from the output?




```
S2# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1,  Fa0/2,  Fa0/3,  Fa0/4
                                                Fa0/5,  Fa0/6,  Fa0/7,  Fa0/8
                                                Fa0/9,  Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20

20   Student                          active    Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

- There is a native VLAN mismatch between the switches.
- There is no media connected to the interfaces.
- They are administratively shut down.
- **They are configured as trunk interfaces.**

Explanation: Interfaces that are configured as trunks do not belong to a VLAN and therefore will not show in the output of the **`show vlan brief`** commands.

Question 21

28. A network contains multiple VLANs spanning multiple switches. What happens when a device in VLAN 20 sends a broadcast Ethernet frame?

- All devices in all VLANs see the frame.
- Devices in VLAN 20 and the management VLAN see the frame.
- **Only devices in VLAN 20 see the frame.**
- Only devices that are connected to the local switch see the frame.

Explanation: VLANs create logical broadcast domains that can span multiple VLAN segments. Ethernet frames that are sent by a device on a specific VLAN can only be seen by other devices in the same VLAN.

Question 22

31. Match the IEEE 802.1Q standard VLAN tag field with the description. (Not all options are used.)

Canonical Format Identifier -- An identifier that enables Token Ring frames to be carried across Ethernet links

VLAN ID -- A VLAN number
User Priority -- A value that supports level or service implementation

Type -- A value for the tag protocol ID value.

Question 23

35. Which command displays the encapsulation type, the voice VLAN ID, and the access mode VLAN for the Fa0/1 interface?

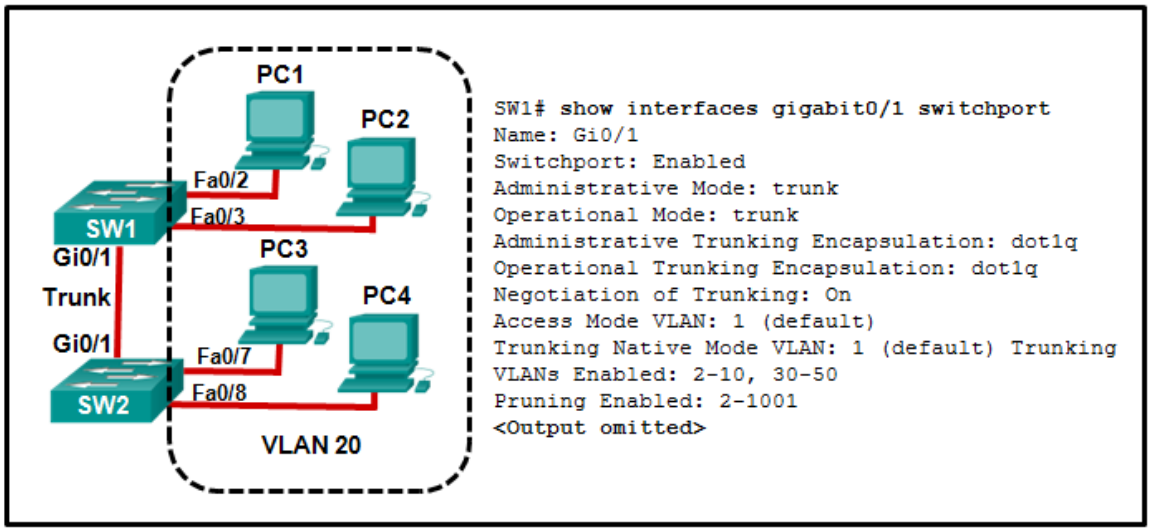
- show vlan brief
- **show interfaces Fa0/1 switchport**
- show mac address-table interface Fa0/1
- show interfaces trunk

Explanation: The **`show interfaces switchport`** command displays the following information for a given port:
Switchport
Administrative Mode
Operational Mode
Administrative Trunking Encapsulation
Operational Trunking Encapsulation
Negotiation of Trunking

Access Mode VLAN
Trunking Native Mode VLAN
Administrative Native VLAN tagging
Voice VLAN

Question 24

29. Refer to the exhibit. All workstations are configured correctly in VLAN 20. Workstations that are connected to switch SW1 are not able to send traffic to workstations on SW2. What could be done to remedy the problem?



- **Allow VLAN 20 on the trunk link.**
- Enable DTP on both ends of the trunk.
- Configure all workstations on SW1 to be part of the default VLAN.
- Configure all workstations on SW2 to be part of the native VLAN.

Explanation: Enabling DTP on both switches simply allows negotiation of trunking. The “Negotiation of Trunking” line in the graphic shows that DTP is already enabled. The graphic also shows how the native VLAN is 1, and the default VLAN for any Cisco switch is 1. The graphic shows the PCs are to be in VLAN 20.

Question 25

37. Which four steps are needed to configure a voice VLAN on a switch port? (Choose four).

- Configure the interface as an IEEE 802.1Q trunk.
- **Assign the voice VLAN to the switch port.**
- Activate spanning-tree PortFast on the interface.
- **Ensure that voice traffic is trusted and tagged with a CoS priority value.**
- **Add a voice VLAN.**
- Configure the switch port interface with subinterfaces.
- Assign a data VLAN to the switch port.
- **Configure the switch port in access mode.**

Explanation: To add an IP phone, the following commands should be added to the switch port:

```
SW3(config-vlan)# vlan 150
SW3(config-vlan)# name voice
SW3(config-vlan)# int fa0/20
SW3(config-if)# switchport mode access
SW3(config-if)# mls qos trust cos
SW3(config-if)# switchport access vlan 150
```

Question 26

36. Refer to the exhibit. A technician is programming switch SW3 to manage voice and data traffic through port Fa0/20. What, if anything, is wrong with the configuration?

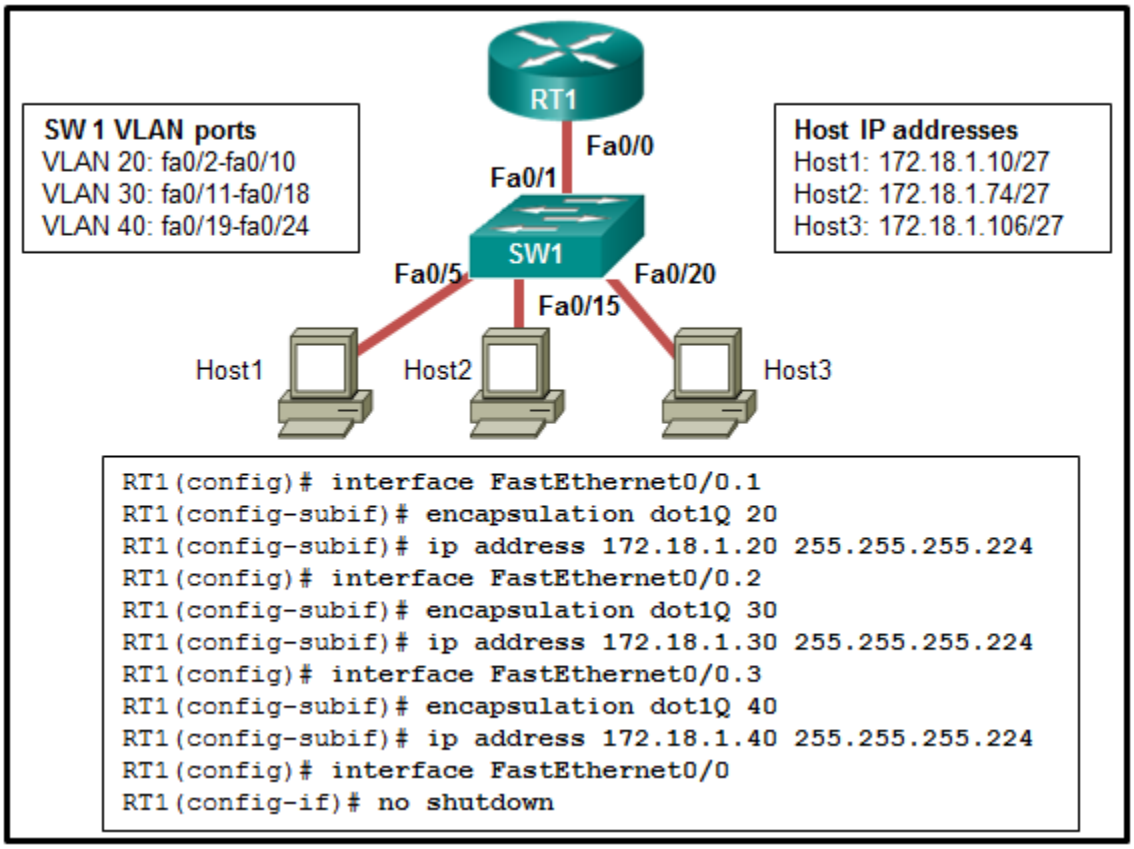
```
SW3(config)# vlan 35
SW3(config-vlan)# name marketing
SW3(config-vlan)# vlan 150
SW3(config-vlan)# name voice
SW3(config-vlan)# int fa0/20
SW3(config-if)# switchport mode access
SW3(config-if)# switchport access vlan 35
SW3(config-if)# mls qos trust cos
SW3(config-if)# switchport access vlan 150
SW3(config-if)# end
```

- There is nothing wrong with the configuration.
- Interface Fa0/20 can only have one VLAN assigned.
- The mls qos trust cos command should reference VLAN 35.
- **The command used to assign the voice VLAN to the switch port is incorrect.**

Explanation: The voice VLAN should be configured with the **`switchport voice vlan 150`** command. A switch interface can be configured to support one data VLAN and one voice VLAN. The **`mls qos trust cos`** associates with the interface. Voice traffic must be trusted so that fields within the voice packet can be used to classify it for QoS.

Question 27

46. Refer to the exhibit. A network administrator is configuring RT1 for inter-VLAN routing. The switch is configured correctly and is functional. Host1, Host2, and Host3 cannot communicate with each other. Based on the router configuration, what is causing the problem?



- Interface Fa0/0 is missing IP address configuration information.
- **IP addresses on the subinterfaces are incorrectly matched to the VLANs.**
- Each subinterface of Fa0/0 needs separate no shutdown commands.
- Routers do not support 802.1Q encapsulation on subinterfaces.

Explanation: Since Host 1 (in VLAN 20) has the IP 172.18.1.10/27, the subinterface Fa0/0.1 should be configured with an IP address in the network 172.168.1.0/27. Similarly, Fa0/0.2 should be with an IP address in the network 172.168.1.64/27 and Fa0/0.3 should be with an IP address in the network 172.168.1.96/27.

Question 28

40. Refer to the exhibit. A network administrator has configured router CiscoVille with the above commands to provide inter-VLAN routing. What command will be required on a switch that is connected to the Gi0/0 interface on router CiscoVille to allow inter-VLAN routing?

```
CiscoVille# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CiscoVille(config)# interface gigabitethernet 0/0
CiscoVille(config-if)# no ip address
CiscoVille(config-if)# interface gigabitethernet 0/0.10
CiscoVille(config-subif)# encapsulation dot1Q 10
CiscoVille(config-subif)# ip address 192.168.10.254 255.255.255.0
CiscoVille(config-subif)# interface gigabitethernet 0/0.20
CiscoVille(config-subif)# encapsulation dot1Q 20
CiscoVille(config-subif)# ip address 192.168.20.254 255.255.255.0
CiscoVille(config-subif)# exit
CiscoVille(config)# interface gigabitethernet 0/0
CiscoVille(config-if)# no shutdown
```

- switchport mode access
- no switchport
- **switchport mode trunk**
- switchport mode dynamic desirable

Explanation: When they are configured for inter-VLAN routing, routers do not support the dynamic trunking protocol that is used by switches. For router-on-a-stick configurations to function, a connected switch must use the command **`switchport mode trunk`**.

Question 29

39. Refer to the exhibit. What is the cause of the error that is displayed in the configuration of inter-VLAN routing on router CiscoVille?

```
CiscoVille# configure terminal
CiscoVille(config)# interface gig0/0
CiscoVille(config-if)# no ip address
CiscoVille(config-if)# interface gig0/0.10
CiscoVille(config-subif)# encapsulation dot1q 10
CiscoVille(config-subif)# ip address 192.168.10.254 255.255.255.0
CiscoVille(config-subif)# interface gig0/0.20
CiscoVille(config-subif)# ip address 192.168.20.254 255.255.255.0

% Configuring IP routing on a LAN subinterface is only allowed if
that subinterface is already configured as part of an IEEE
802.10, IEEE 802.1Q,or ISL vLAN.
```

- The gig0/0 interface does not support inter-VLAN routing.
- The no shutdown command has not been configured.
- The IP address on CiscoVille is incorrect.
- **The encapsulation dot1Q 20 command has not been configured.**

Explanation: ?

Question 30

41. A high school uses VLAN15 for the laboratory network and VLAN30 for the faculty network. What is required to enable communication between these two VLANs while using the router-on-a-stick approach?

- A multilayer switch is needed.
- A router with at least two LAN interfaces is needed.
- Two groups of switches are needed, each with ports that are configured for one VLAN.
- **A switch with a port that is configured as a trunk is needed when connecting to the router.**

Explanation: With router-on-a-stick, inter-VLAN routing is performed by a router with a single router interface that is connected to a switch port configured with trunk mode. Multiple subinterfaces, each configured for a

VLAN, can be configured under the single physical router interface. Switches can have ports that are assigned to different VLANs, but communication between those VLANs requires routing function from the router. A multilayer switch is not used in a router-on-a-stick approach to inter-VLAN routing.

Question 31

42. When routing a large number of VLANs, what are two disadvantages of using the router-on-a-stick inter-VLAN routing method rather than the multilayer switch inter-VLAN routing method? (Choose two.)

- Multiple SVIs are needed.
- **A dedicated router is required.**
- Router-on-a-stick requires subinterfaces to be configured on the same subnets.
- Router-on-a-stick requires multiple physical interfaces on a router.
- **Multiple subinterfaces may impact the traffic flow speed.**

Explanation: With the router-on-a-stick inter-VLAN routing method, a dedicated router is required. It only needs one physical interface on the router to route traffic among multiple VLANs, by using subinterfaces on one physical interface. On the other hand, since traffic of all VLANs will have to go through the same physical interfaces, the throughput will be impacted. Also, a multilayer switch can use multiple SVIs to perform inter-VLAN routing.

Question 32

54. A technician is configuring a new Cisco 2960 switch. What is the effect of issuing the `BranchSw(config-if)# shutdown` command?

- **It disables a virtual or physical switch interface.**
- It saves the running configuration to NVRAM.
- It activates a virtual or physical switch interface.
- It updates the MAC address table for the associated port.
- It saves the startup configuration to the running configuration.

Explanation: ?

Question 33

64. What type of VLAN is designed to have a delay of less than 150 ms across the network?

- **voice VLAN**
- desirable VLAN
- trunk VLAN
- security VLAN

Explanation: ?

You have scored **100%**.

Congratulations, you have passed the exam.

You have used 1 of 1 attempts.

Review Assessment

Here is how you performed in each of the Learning Objectives and Skills associated with this assessment.

Basic Device Management. Initial Device Config. Security 100%

Switching. Switching Fundamentals. Operation 100%

Switching. Switching Fundamentals. VLANs 100%

Routing. Inter-VLAN. Subinterface 100%